(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10020780 A**

(43) Date of publication of application: **23.01.98**

(51) Int. Cl **G09C 1/00**
G09C 1/00
H04L 9/32

(21) Application number: **08168965**

(22) Date of filing: **28.06.96**

(71) Applicant: **SONY CORP**

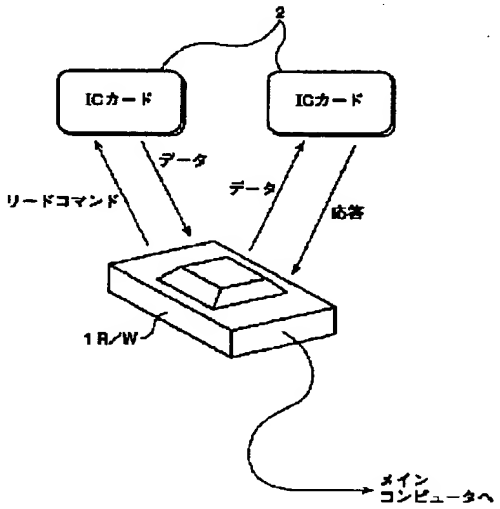
(72) Inventor: **KUSAKABE SUSUMU**
TAKADA MASAYUKI

(54) CERTIFICATION METHOD, COMMUNICATION METHOD AND INFORMATION PROCESSING DEVICE

(57) Abstract:

PROBLEM TO BE SOLVED: To perform the certification mutually, by enciphering a clear text mutually received, to transmit the same to a device which has transmitted the clear text, and comparing the clear text obtained by decoding the received cipher text, with the clear text which has been transmitted first.

SOLUTION: A reader writer(R/W) 1 enciphers random numbers RA to a cipher C_1 with a key KLB, and an IC card 2 encodes the cipher C_1 to a clear text M_1 with the key KB. The IC card 2 enciphers the clear text M_1 to a cipher C_2 with a key KA, the random number RB is enciphered to a cipher C_3 with the key KA, and R/W 1 encodes the cipher C_2 to the clear text M_2 with the key KA. And the R/W 1 certifies the IC card 2 when the clear text M_2 and the random number RA are judged to be same as each other. In the next, R/W 1 encodes the cipher C_3 to a clear text M_3 with the key KA, the clear text M_3 is encoded to a cipher C_4 with the key KB, and the IC card 2 encodes the cipher C_4 to the clear text M_4 with the key KB. And the IC card 2 certifies R/W1, when the clear text M_4 and the random number RB are judged to be same as each other.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－20780

(43)公開日　平成10年(1998) 1月23日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０９Ｃ	1/00	６４０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６４０Ａ
			7259－5Ｊ			６４０Ｅ
		６６０	7259－5Ｊ			６６０Ａ
Ｈ０４Ｌ	9/32			Ｈ０４Ｌ	9/00	６７５Ａ

審査請求　未請求　請求項の数30　ＯＬ　（全 18 頁）

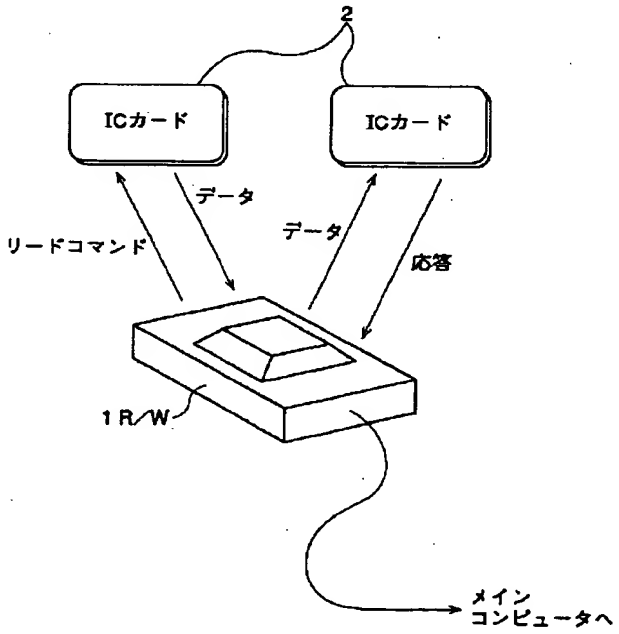
(21)出願番号　特願平8－168965

(22)出願日　平成８年(1996) ６月28日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　日下部　進
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　高田　昌幸
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　弁理士　稲本　義雄

(54)【発明の名称】　認証方法、通信方法、および、情報処理装置

(57)【要約】
【課題】　相互に認証を行う。
【解決手段】　Ｒ／Ｗ１は、乱数R_Aを鍵K_Bで暗号化した暗号C_1をＩＣカード２に送信する。ＩＣカード２は、その暗号C_1を鍵K_Bで平文M_1に復号化する。ＩＣカード２は、平文M_1を鍵K_Aで暗号化した暗号C_2と、乱数R_Bを鍵K_Aで暗号化した暗号C_3をＲ／Ｗ１に送信する。Ｒ／Ｗ１は、その暗号C_2，C_3を、鍵K_Aで平文M_2と平文M_3にそれぞれ復号化する。Ｒ／Ｗ１は、平文M_2と乱数R_Aが同一であると判断した場合、ＩＣカード２を認証する。次に、Ｒ／Ｗ１は、平文M_3を鍵K_Bで暗号化した暗号C_4をＩＣカード２に送信する。ＩＣカード２は、その暗号C_4を、鍵K_Bで平文M_4に復号化する。ＩＣカード２は、平文M_4と乱数R_Bが同一であると判断した場合、Ｒ／Ｗ１を認証する。



1

【特許請求の範囲】

【請求項１】　第１の鍵および第２の鍵を記憶する記憶手段と、

所定のデータを前記第１の鍵または前記第２の鍵を利用して暗号化する暗号化手段と、

前記第２の鍵または前記第１の鍵による暗号を復号化する復号化手段とをそれぞれ備える第１の情報処理装置と第２の情報処理装置との間における認証方法において、

前記第１の情報処理装置の前記暗号化手段が、前記第１の鍵で、第１のデータを第１の暗号に暗号化するステップと、

前記第２の情報処理装置の前記復号化手段が、前記第１の鍵で、前記第１の暗号を第２のデータに復号化するステップと、

前記第２の情報処理装置の前記暗号化手段が、前記第２の鍵で、前記第２のデータを第２の暗号に暗号化するステップと、

前記第２の情報処理装置の前記暗号化手段が、前記第２の鍵で、第３のデータを第３の暗号に暗号化するステップと、

前記第１の情報処理装置の前記復号化手段が、前記第２の鍵で、前記第２の暗号を第４のデータに復号化するステップと、

前記第１の情報処理装置が、前記第１のデータと前記第４のデータに応じて、前記第２の情報処理装置を認証するステップと、

前記第１の情報処理装置の前記復号化手段が、前記第２の鍵で、前記第３の暗号を第５のデータに復号化するステップと、

前記第１の情報処理装置の前記暗号化手段が、前記第１の鍵で、前記第５のデータを第４の暗号に暗号化するステップと、

前記第２の情報処理装置の前記復号化手段が、前記第１の鍵で、前記第４の暗号を第６のデータに復号化するステップと、

前記第２の情報処理装置が、前記第３のデータと前記第６のデータに応じて、前記第１の情報処理装置を認証するステップとを備えることを特徴とする認証方法。

【請求項２】　第１の鍵および第２の鍵を記憶する記憶手段と、

所定のデータを前記第１の鍵または前記第２の鍵を利用して暗号化する暗号化手段と、

前記第２の鍵または前記第１の鍵による暗号を復号化する復号化手段と、

暗号化された前記データを送信する送信手段と、

所定の暗号化されたデータを受信する受信手段とを備える第１の情報処理装置と第２の情報処理装置との間における通信方法において、

前記第１の情報処理装置の前記暗号化手段が、前記第１の鍵で、第１のデータを第１の暗号に暗号化するステップと、

前記第１の情報処理装置の前記送信手段が、前記第１の暗号を、前記第２の情報処理装置に送信するステップと、

前記第２の情報処理装置の前記受信手段が、前記第１の暗号を受信するステップと、

前記第２の情報処理装置の前記復号化手段が、前記第１の鍵で、前記第１の暗号を第２のデータに復号化するステップと、

前記第２の情報処理装置の前記暗号化手段が、前記第２の鍵で、前記第２のデータを第２の暗号に暗号化するステップと、

前記第２の情報処理装置の前記暗号化手段が、前記第２の鍵で、第３のデータを第３の暗号に暗号化するステップと、

前記第２の情報処理装置の前記送信手段が、前記第２の暗号および前記第３の暗号を、前記第１の情報処理装置に送信するステップと、

前記第１の情報処理装置の前記受信手段が、前記第２の暗号および前記第３の暗号を受信するステップと、

前記第１の情報処理装置の前記復号化手段が、前記第２の鍵で、前記第２の暗号を第４のデータに復号化するステップと、

前記第１の情報処理装置が、前記第１のデータと前記第４のデータに応じて、前記第２の情報処理装置を認証するステップと、

前記第１の情報処理装置の前記復号化手段が、前記第２の鍵で、前記第３の暗号を第５のデータに復号化するステップと、

前記第１の情報処理装置の前記暗号化手段が、前記第１の鍵で、前記第５のデータを第４の暗号に暗号化するステップと、

前記第１の情報処理装置の前記送信手段が、前記第４の暗号を、前記第２の情報処理装置に送信するステップと、

前記第２の情報処理装置の前記受信手段が、前記第４の暗号を受信するステップと、

前記第２の情報処理装置の前記復号化手段が、前記第１の鍵で、前記第４の暗号を第６のデータに復号化するステップと、

前記第２の情報処理装置が、前記第３のデータと前記第６のデータに応じて、前記第１の情報処理装置を認証するステップとを備えることを特徴とする通信方法。

【請求項３】　前記第１のデータは、所定の認識番号であり、

前記第３のデータは、第３の鍵であり、

前記第１の情報処理装置の前記暗号化手段は、第１のコマンドを、前記第３の鍵で第５の暗号に暗号化するとともに、前記認識番号を、前記第３の鍵で第６の暗号に暗号化し、

前記第１の情報処理装置の前記送信手段は、前記第５の暗号を、前記第６の暗号とともに送信し、

前記第２の情報処理装置の前記受信手段は、前記第５の暗号および前記第６の暗号を受信し、

前記第２の情報処理装置の前記復号化手段は、前記第５の暗号を、前記第３の鍵で第２のコマンドに復号化するとともに、前記第６の暗号を、前記第３の鍵で第７のデータに復号化し、

前記第２の情報処理装置は、前記第７のデータと前記認識番号の値に応じて、前記第２のコマンドを承認することを特徴とする請求項２に記載の通信方法。

【請求項４】　前記第１の情報処理装置の前記認識番号は、前記第１のコマンドの暗号化毎に変更されることを特徴とする請求項３に記載の通信方法。

【請求項５】　前記第１の情報処理装置の前記認識番号は、前記第１のコマンドの暗号化毎に増加されることを特徴とする請求項４に記載の通信方法。

【請求項６】　前記第２の情報処理装置は、前記第７のデータが前記認識番号に対応する所定の範囲内の値であるとき、前記第２のコマンドを承認することを特徴とする請求項３に記載の通信方法。

【請求項７】　前記第２の情報処理装置は、前記第７のデータと前記認識番号の値を所定の桁数の範囲だけにおいて比較し、前記第７のデータにおける前記所定の桁数の範囲の値が、前記認識番号における前記所定の桁数の範囲の値以上であるとき、前記第２のコマンドを承認することを特徴とする請求項３に記載の通信方法。

【請求項８】　前記第２の情報処理装置は、前記第２のコマンドに対応する処理を行い、その処理の結果に対応する応答データを生成し、

前記第２の情報処理装置の前記暗号化手段は、前記応答データを、前記第３の鍵で第７の暗号に暗号化するとともに、前記認識番号を、前記第３の鍵で第８の暗号に暗号化し、

前記第２の情報処理装置の前記送信手段は、前記第７の暗号を、前記第８の暗号とともに送信し、

前記第１の情報処理装置の前記受信手段は、前記第７の暗号および前記第８の暗号を受信し、

前記第１の情報処理装置の前記復号化手段は、前記第７の暗号を、前記第３の鍵で第８のデータに復号化するとともに、前記第８の暗号を、前記第３の鍵で第９のデータに復号化し、

前記第１の情報処理装置は、前記第９のデータと前記認識番号の値に応じて、前記第８のデータを、前記応答データとして承認することを特徴とする請求項３に記載の通信方法。

【請求項９】　前記第２の情報処理装置の前記認識番号は、前記第８のデータの暗号化毎に変更されることを特徴とする請求項８に記載の通信方法。

【請求項１０】　前記第２の情報処理装置の前記認識番号は、前記第８のデータの暗号化毎に増加されることを特徴とする請求項９に記載の通信方法。

【請求項１１】　前記第１の情報処理装置は、前記第９のデータが前記認識番号に対応する所定の範囲内の値であるとき、前記第８のデータを、前記応答データとして承認することを特徴とする請求項８に記載の通信方法。

【請求項１２】　前記第１の情報処理装置は、前記第９のデータと前記認識番号の値を所定の桁数の範囲だけにおいて比較し、前記第９のデータにおける前記所定の桁数の範囲の値が、前記認識番号における前記所定の桁数の範囲の値以上であるとき、前記第８のデータを、前記応答データとして承認することを特徴とする請求項８に記載の通信方法。

【請求項１３】　前記第１の情報処理装置は、前記第５の暗号を、前記第６の暗号とともに送信した後、前記７の暗号および前記第８の暗号を受信するまでに所定の時間が経過した場合、前記認識番号の値を増加した後、前記認識番号を前記第６の暗号に暗号化し、前記第５の暗号を、前記第６の暗号とともに再送することを特徴とする請求項８に記載の通信方法。

【請求項１４】　前記第１の情報処理装置は、前記第８のデータを、応答データとして承認しない場合、前記認識番号の値を増加した後、前記認識番号を前記第６の暗号に暗号化し、前記第５の暗号を、前記第６の暗号とともに再送することを特徴とする請求項８に記載の通信方法。

【請求項１５】　第１の鍵および第２の鍵を記憶する記憶手段と、

所定のデータを、前記第１の鍵または前記第２の鍵を利用して暗号化する暗号化手段と、

前記第２の鍵または前記第１の鍵による暗号を復号化する復号化手段と、

前記暗号化手段により暗号化された暗号を他の情報処理装置に送信する送信手段と、

前記他の情報処理装置から暗号を受信する受信手段とを備える情報処理装置において、

前記所定のデータと、前記他の情報処理装置から受信した暗号を復号化して生成されたデータに応じて、前記他の情報処理装置を認証する認証手段をさらに備え、

前記暗号化手段が、前記第１の鍵で、第１のデータを第１の暗号に暗号化し、

前記送信手段が、前記第１の暗号を前記他の情報処理装置に送信し、

前記受信手段が、前記他の情報処理装置から、第２の暗号および第３の暗号を受け取り、

前記復号化手段が、前記第２の暗号を、前記第２の鍵で第４のデータに復号化するとともに、前記第３の暗号を、前記第２の鍵で第５のデータに復号化し、

前記認証手段が、前記第１のデータと前記第４のデータに応じて、前記他の情報処理装置を認証し、

前記暗号化手段が、前記第５のデータを、前記第１の鍵で第４の暗号に暗号化し、
前記送信手段が、前記第４の暗号を前記他の情報処理装置に送信することを特徴とする情報処理装置。
【請求項１６】　前記第１のデータは、所定の認識番号であり、
前記第５のデータは、第３の鍵であり、
前記暗号化手段は、第１のコマンドを、前記第３の鍵で第５の暗号に暗号化するとともに、前記認識番号を、前記第３の鍵で第６の暗号に暗号化し、
前記送信手段は、前記第５の暗号を、前記第６の暗号とともに、前記他の情報処理装置に送信することを特徴とする請求項１５に記載の情報処理装置。
【請求項１７】　前記受信手段は、前記他の情報処理装置から前記第１のコマンドに対応する処理の結果に対応する応答データを暗号化した第７の暗号と、前記他の情報処理装置における前記認識番号を暗号化した第８の暗号を受信し、
前記復号化手段は、前記第７の暗号を、前記第３の鍵で第８のデータに復号化するとともに、前記第８の暗号を、前記第３の鍵で第９のデータに復号化し、
前記認証手段は、前記第９のデータと前記認識番号の値に応じて、前記第８のデータを、前記応答データとして承認することを特徴とする請求項１６に記載の情報処理装置。
【請求項１８】　前記認識番号は、前記第１のコマンドの暗号化毎に変更されることを特徴とする請求項１６に記載の情報処理装置。
【請求項１９】　前記認識番号は、前記第１のコマンドの暗号化毎に増加されることを特徴とする請求項１８に記載の情報処理装置。
【請求項２０】　前記認証手段は、前記第９のデータが前記認識番号に対応する所定の範囲内の値であるとき、前記第８のデータを、前記応答データとして承認することを特徴とする請求項１７に記載の情報処理装置。
【請求項２１】　前記認証手段は、前記第９のデータと前記認識番号の値を所定の桁数の範囲だけにおいて比較し、前記第９のデータにおける前記所定の桁数の範囲の値が、前記認識番号における前記所定の桁数の範囲の値以上であるとき、前記第８のデータを、前記応答データとして承認することを特徴とする請求項２０に記載の情報処理装置。
【請求項２２】　前記第５の暗号を、前記第６の暗号とともに送信した後、前記７の暗号および第８の暗号を受信するまでに所定の時間が経過した場合、前記認識番号の値を増加した後、前記認識番号を前記第６の暗号に暗号化し、前記第５の暗号を、前記第６の暗号とともに再送することを特徴とする請求項１７に記載の情報処理装置。
【請求項２３】　前記認証手段が前記第８のデータを応答データとして承認しない場合、前記認識番号の値を増加した後、前記認識番号を前記第６の暗号に暗号化し、前記第５の暗号を、前記第６の暗号とともに再送することを特徴とする請求項１７に記載の情報処理装置。

【請求項２４】　第１の鍵および第２の鍵を記憶する記憶手段と、
所定のデータを、前記第１の鍵または前記第２の鍵を利用して暗号化する暗号化手段と、
前記第２の鍵または前記第１の鍵による暗号を復号化する復号化手段と、
前記暗号化手段により暗号化された暗号を他の情報処理装置に送信する送信手段と、
前記他の情報処理装置から暗号を受信する受信手段とを備える情報処理装置において、
前記所定のデータと、前記他の情報処理装置から受信した暗号を復号化して得られたデータに応じて、前記他の情報処理装置を認証する認証手段をさらに備え、
前記受信手段が、前記他の情報処理装置より第１の暗号を受け取り、
前記復号化手段が、前記第１の暗号を、前記第１の鍵で第２のデータに復号化し、
前記暗号化手段が、前記第２のデータを、前記第２の鍵で第２の暗号に暗号化するとともに、第３のデータを、前記第２の鍵で第３の暗号に暗号化し、
前記送信手段が、前記第２の暗号および前記第３の暗号を前記他の情報処理装置に送信し、
前記受信手段が、前記他の情報処理装置から第４の暗号を受け取り、
前記復号化手段が、前記第４の暗号を、前記第２の鍵で第６のデータに復号化し、
前記認証手段が、前記第３のデータと前記第６のデータに応じて、前記他の情報処理装置を認証することを特徴とする情報処理装置。
【請求項２５】　前記第２のデータは、所定の認識番号であり、
前記第３のデータは、第３の鍵であり、
前記受信手段は、前記他の情報処理装置から、第１のコマンドを前記第３の鍵で暗号化した第５の暗号と、前記他の情報処理装置の前記認識番号を暗号化した第６の暗号を受信し、
前記復号化手段は、前記第５の暗号を、前記第３の鍵で第２のコマンドに復号化するとともに、前記第６の暗号を、前記第３の鍵で第７のデータに復号化し、
前記認証手段は、前記第７のデータと前記認識番号の値に応じて、前記第２のコマンドを承認することを特徴とする請求項２４に記載の情報処理装置。
【請求項２６】　前記第２のコマンドに対応する処理を行い、その処理の結果に対応する応答データを生成する処理手段をさらに備え、
前記暗号化手段は、前記応答データを、前記第３の鍵で

第７の暗号に暗号化するとともに、前記認識番号を、前記第３の鍵で第８の暗号に暗号化し、
前記送信手段は、前記第７の暗号を、前記第８の暗号とともに送信することを特徴とする請求項２５に記載の情報処理装置。
【請求項２７】　前記認識番号は、前記第７の暗号の暗号化毎に変更されることを特徴とする請求項２６に記載の情報処理装置。
【請求項２８】　前記認識番号は、前記第７の暗号の暗号化毎に増加されることを特徴とする請求項２７に記載の情報処理装置。
【請求項２９】　前記認証手段は、前記第７のデータが、前記認識番号に対応する所定の範囲内の値であるとき、前記第２のコマンドを承認することを特徴とする請求項２５に記載の情報処理装置。
【請求項３０】　前記認証手段は、前記第７のデータと前記認識番号の値を所定の桁数の範囲だけにおいて比較し、前記第７のデータにおける前記所定の桁数の範囲の値が、前記認識番号における前記所定の桁数の範囲の値以上であるとき、前記第２のコマンドを承認することを特徴とする請求項２５に記載の情報処理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、認証方法、通信方法、および、情報処理装置に関し、特に、複数の情報処理装置が相互に認証を行う認証方法、通信方法、および、情報処理装置に関する。
【０００２】
【従来の技術】情報処理技術の発展に伴い、大量の情報が所定の伝送路を介して通信されている。情報が通信される伝送路には、第三者（送信者および受信者以外の者）が、通信されているデータを盗聴することが可能なものが多い。
【０００３】このような伝送路を利用して、情報を第三者に漏洩させずに、通信を行う場合、しばしば、暗号が利用される。暗号を利用し、暗号化されたデータを通信することにより、暗号化されたデータを盗聴することができても、第三者が、そのデータから通信した情報の内容を読み出すことは困難である。
【０００４】このような暗号を生成する暗号化方法には、所定の鍵を利用して、平文（送信する情報）から、暗号（実際に送信されるデータ）を生成するものが利用されることが多い。
【０００５】このような、鍵を利用した暗号には、共通鍵暗号と公開鍵暗号の２種類がある。共通鍵暗号においては、暗号化するときの鍵（暗号化鍵データ）と、復号化するときの鍵（復号化鍵データ）が同一である。例えば、共通鍵暗号としては、Feistel暗号の１つであるＤＥＳ（Data Encryption Standard）方式などがよく利用されている。一方、公開鍵暗号においては、暗号化鍵データと復号化鍵データが異なる。そして、受信者は、送信者のために、それらの鍵のうち、暗号化鍵データを公開するが、復号化鍵データは公開せずに隠しておく（即ち、復号化鍵データは、受信者のみが知っている）。
【０００６】図１４は、このような鍵（共通鍵）を利用した通信（秘密通信）の一例を示している。送信者１０１は、送信する情報（平文Ｍ）を、鍵Ｋを利用して暗号Ｃに暗号化する。そして、送信者１０１は、暗号Ｃを、所定の伝送路を介して受信者１０２に送信する。
【０００７】受信者１０２は、暗号Ｃを受け取り、送信者１０１が有する鍵Ｋと同一の鍵Ｋを利用して、その暗号Ｃを復号化し、送信者１０１により送信された情報（平文Ｍ）を獲得する。
【０００８】このようにして通信が行われているとき、暗号Ｃを盗聴しても、第三者が、送信された情報（平文Ｍ）を獲得することは困難である。
【０００９】さらに、このような鍵を利用して、通信相手が、正規の受信者であるか否かを判断する（認証する）ことができる。図１５は、鍵（共通鍵）を利用した認証の一例を示している。認証する側１１１は、乱数Ｍを発生し、その乱数Ｍを認証される側１１２に送信する。認証する側１１１は、認証される側１１２に、その乱数Ｍを、鍵Ｋで暗号Ｃに暗号化させ、その暗号Ｃを送信させる。そして、認証する側１１１は、その暗号Ｃを受信し、鍵Ｋで平文Ｍ１に復号化する。そして、認証する側１１１は、乱数Ｍと平文Ｍ１が一致するか否かを判断し、一致する場合、認証される側１１２を認証する。
【００１０】このようにして、送信者（認証する側１１１）は、受信者（認証される側１１２）が正規の受信者（送信者が有する鍵と同一の鍵を有する）であるか否かを判断する（認証する）ことができる。
【００１１】このとき、平文である乱数Ｍと、それを暗号化した暗号Ｃを、第三者が盗聴したとしても、平文Ｍと暗号Ｃから、鍵Ｋを生成することは困難であるので、送信者（認証する側１１１）の鍵Ｋと同一の鍵Ｋを有する正規の受信者のみが認証される。
【００１２】
【発明が解決しようとする課題】しかしながら、上述の認証方法においては、所定の送受信者が、他の送受信者を認証するだけであるので、例えば、リーダ／ライタ（Ｒ／Ｗ）とＩＣカードで構成されるカードシステムに、上述の認証方法を適用した場合、Ｒ／Ｗは、通信相手が正規のＩＣカードであるか否かを判断する（通信相手を認証する）ことができるが、ＩＣカードは、通信相手が正規のＲ／Ｗであるか否かを判断することが困難であるという問題を有している。
【００１３】本発明は、このような状況に鑑みてなされたものであり、複数の情報処理装置において、相互に平文を送信するとともに、送信されてきた平文を受信し、受信した平文を暗号に暗号化し、平文を送信した装置

に、その暗号を送信するとともに、送信されてきた暗号を受信し、その暗号を復号化した平文と最初に送信した平文を比較することで、相互に認証を行うようにするものである。

【００１４】

【課題を解決するための手段】請求項１に記載の認証方法は、第１の情報処理装置の暗号化手段が、第１の鍵で、第１のデータを第１の暗号に暗号化するステップと、第２の情報処理装置の復号化手段が、第１の鍵で、第１の暗号を第２のデータに復号化するステップと、第２の情報処理装置の暗号化手段が、第２の鍵で、第２のデータを第２の暗号に暗号化するステップと、第２の情報処理装置の暗号化手段が、第２の鍵で、第３のデータを第３の暗号に暗号化するステップと、第１の情報処理装置の復号化手段が、第２の鍵で、第２の暗号を第４のデータに復号化するステップと、第１の情報処理装置が、第１のデータと第４のデータに応じて、第２の情報処理装置を認証するステップと、第１の情報処理装置の復号化手段が、第２の鍵で、第３の暗号を第５のデータに復号化するステップと、第１の情報処理装置の暗号化手段が、第１の鍵で、第５のデータを第４の暗号に暗号化するステップと、第２の情報処理装置の復号化手段が、第１の鍵で、第４の暗号を第６のデータに復号化するステップと、第２の情報処理装置が、第３のデータと第６のデータに応じて、第１の情報処理装置を認証するステップとを備えることを特徴とする。

【００１５】請求項２に記載の通信方法は、第１の情報処理装置の暗号化手段が、第１の鍵で、第１のデータを第１の暗号に暗号化するステップと、第１の情報処理装置の送信手段が、第１の暗号を、第２の情報処理装置に送信するステップと、第２の情報処理装置の受信手段が、第１の暗号を受信するステップと、第２の情報処理装置の復号化手段が、第１の鍵で、第１の暗号を第２のデータに復号化するステップと、第２の情報処理装置の暗号化手段が、第２の鍵で、第２のデータを第２の暗号に暗号化するステップと、第２の情報処理装置の暗号化手段が、第２の鍵で、第３のデータを第３の暗号に暗号化するステップと、第２の情報処理装置の送信手段が、第２の暗号および第３の暗号を、第１の情報処理装置に送信するステップと、第１の情報処理装置の受信手段が、第２の暗号および第３の暗号を受信するステップと、第１の情報処理装置の復号化手段が、第２の鍵で、第２の暗号を第４のデータに復号化するステップと、第１の情報処理装置が、第１のデータと第４のデータに応じて、第２の情報処理装置を認証するステップと、第１の情報処理装置の復号化手段が、第２の鍵で、第３の暗号を第５のデータに復号化するステップと、第１の情報処理装置の暗号化手段が、第１の鍵で、第５のデータを第４の暗号に暗号化するステップと、第１の情報処理装置の送信手段が、第４の暗号を、第２の情報処理装置に送信するステップと、第２の情報処理装置の受信手段が、第４の暗号を受信するステップと、第２の情報処理装置の復号化手段が、第１の鍵で、第４の暗号を第６のデータに復号化するステップと、第２の情報処理装置が、第３のデータと第６のデータに応じて、第１の情報処理装置を認証するステップとを備えることを特徴とする。

【００１６】請求項１５に記載の情報処理装置は、所定のデータと、他の情報処理装置から受信した暗号を復号化して生成されたデータに応じて、他の情報処理装置を認証する認証手段をさらに備え、暗号化手段が、第１の鍵で、第１のデータを第１の暗号に暗号化し、送信手段が、第１の暗号を他の情報処理装置に送信し、受信手段が、他の情報処理装置から、第２の暗号および第３の暗号を受け取り、復号化手段が、第２の暗号を、第２の鍵で第４のデータに復号化するとともに、第３の暗号を、第２の鍵で第５のデータに復号化し、認証手段が、第１のデータと第４のデータに応じて、他の情報処理装置を認証し、暗号化手段が、第５のデータを、第１の鍵で第４の暗号に暗号化し、送信手段が、第４の暗号を他の情報処理装置に送信することを特徴とする。

【００１７】請求項２４に記載の情報処理装置は、所定のデータと、他の情報処理装置から受信した暗号を復号化して得られたデータに応じて、他の情報処理装置を認証する認証手段をさらに備え、受信手段が、他の情報処理装置により第１の暗号を受け取り、復号化手段が、第１の暗号を、第１の鍵で第１のデータに復号化し、暗号化手段が、第１のデータを、第２の鍵で第２の暗号に暗号化するとともに、第２のデータを、第２の鍵で第３の暗号に暗号化し、送信手段が、第２の暗号および第３の暗号を他の情報処理装置に送信し、受信手段が、他の情報処理装置から第４の暗号を受け取り、復号化手段が、第４の暗号を、第２の鍵で第３のデータに復号化し、認証手段が、第２のデータと第３のデータに応じて、他の情報処理装置を認証することを特徴とする。

【００１８】請求項１に記載の認証方法においては、第１の情報処理装置の暗号化手段が、第１の鍵で、第１のデータを第１の暗号に暗号化し、第２の情報処理装置の復号化手段が、第１の鍵で、第１の暗号を第２のデータに復号化し、第２の情報処理装置の暗号化手段が、第２の鍵で、第２のデータを第２の暗号に暗号化し、第２の情報処理装置の暗号化手段が、第２の鍵で、第３のデータを第３の暗号に暗号化し、第１の情報処理装置の復号化手段が、第２の鍵で、第２の暗号を第４のデータに復号化し、第１の情報処理装置が、第１のデータと第４のデータに応じて、第２の情報処理装置を認証し、第１の情報処理装置の復号化手段が、第２の鍵で、第３の暗号を第５のデータに復号化し、第１の情報処理装置の暗号化手段が、第１の鍵で、第５のデータを第４の暗号に暗号化し、第２の情報処理装置の復号化手段が、第１の鍵

で、第４の暗号を第６のデータに復号化し、第２の情報処理装置が、第３のデータと第６のデータに応じて、第１の情報処理装置を認証する。

【００１９】請求項２に記載の通信方法においては、第１の情報処理装置の暗号化手段が、第１の鍵で、第１のデータを第１の暗号に暗号化し、第１の情報処理装置の送信手段が、第１の暗号を、第２の情報処理装置に送信し、第２の情報処理装置の受信手段が、第１の暗号を受信し、第２の情報処理装置の復号化手段が、第１の鍵で、第１の暗号を第２のデータに復号化し、第２の情報処理装置の暗号化手段が、第２の鍵で、第２のデータを第２の暗号に暗号化し、第２の情報処理装置の暗号化手段が、第２の鍵で、第３のデータを第３の暗号に暗号化し、第２の情報処理装置の送信手段が、第２の暗号および第３の暗号を、第１の情報処理装置に送信し、第１の情報処理装置の受信手段が、第２の暗号および第３の暗号を受信し、第１の情報処理装置の復号化手段が、第２の鍵で、第２の暗号を第４のデータに復号化し、第１の情報処理装置が、第１のデータと第４のデータに応じて、第２の情報処理装置を認証し、第１の情報処理装置の復号化手段が、第２の鍵で、第３の暗号を第５のデータに復号化し、第１の情報処理装置の暗号化手段が、第１の鍵で、第５のデータを第４の暗号に暗号化し、第１の情報処理装置の送信手段が、第４の暗号を、第２の情報処理装置に送信し、第２の情報処理装置の受信手段が、第４の暗号を受信し、第２の情報処理装置の復号化手段が、第１の鍵で、第４の暗号を第６のデータに復号化し、第２の情報処理装置が、第３のデータと第６のデータに応じて、第１の情報処理装置を認証する。

【００２０】請求項１５に記載の情報処理装置においては、暗号化手段が、第１の鍵で、第１のデータを第１の暗号に暗号化し、送信手段が、第１の暗号を他の情報処理装置に送信し、受信手段が、他の情報処理装置から、第２の暗号および第３の暗号を受け取り、復号化手段が、第２の暗号を、第２の鍵で第４のデータに復号化するとともに、第３の暗号を、第２の鍵で第５のデータに復号化し、認証手段が、第１のデータと第４のデータに応じて、他の情報処理装置を認証し、暗号化手段が、第５のデータを、第１の鍵で第４の暗号に暗号化し、送信手段が、第４の暗号を他の情報処理装置に送信する。

【００２１】請求項２４に記載の情報処理装置においては、受信手段が、他の情報処理装置により第１の暗号を受け取り、復号化手段が、第１の暗号を、第１の鍵で第１のデータに復号化し、暗号化手段が、第１のデータを、第２の鍵で第２の暗号に暗号化するとともに、第２のデータを、第２の鍵で第３の暗号に暗号化し、送信手段が、第２の暗号および第３の暗号を他の情報処理装置に送信し、受信手段が、他の情報処理装置から第４の暗号を受け取り、復号化手段が、第４の暗号を、第２の鍵で第３のデータに復号化し、認証手段が、第２のデータと第３のデータに応じて、他の情報処理装置を認証する。

【００２２】

【発明の実施の形態】図１は、Ｒ／Ｗ１およびＩＣカード２を利用した非接触カードシステムの一例を示している。Ｒ／Ｗ１およびＩＣカード２は、電磁波を利用して非接触で、データの送受信を行う。

【００２３】例えば、Ｒ／Ｗ１が、リードコマンドをＩＣカード２に送信すると、ＩＣカード２は、そのリードコマンドを受信し、リードコマンドで指示されたデータをＲ／Ｗ１に送信するようになされている。

【００２４】また、Ｒ／Ｗ１がデータをＩＣカード２に送信すると、ＩＣカード２は、そのデータを受信し、受信したデータを、内蔵するメモリ８４（図６）（記憶手段）に記憶し、そのデータを記憶したことを表す所定の応答信号をＲ／Ｗ１に送信するようになされている。

【００２５】図２は、本発明の一実施例であるＲ／Ｗ１の構成を示している。

【００２６】Ｒ／Ｗ１においては、制御部１１は、内蔵するプログラムに応じて、各種処理を行うようになされている。例えば、制御部１１は、ＩＣカード２に送信するデータを、暗号部１２（暗号化手段）に出力するとともに、復号部１３（復号化手段）より供給された、ＩＣカード２からの応答データを処理するようになされている。

【００２７】また、制御部１１は、メモリ１４（記憶手段）から、暗号化または復号化に利用される鍵K_A（第２の鍵）または鍵K_B（第１の鍵）を読み出し、その鍵K_Aまたは鍵K_Bを、暗号部１２または復号部１３に出力するようになされている。

【００２８】さらに、制御部１１は、インタフェース１５を介して、メインコンピュータ（図示せず）と通信を行うようになされている。

【００２９】メモリ１４は、制御部１１における処理に使用されるデータなどを記憶している他、暗号化または復号化において利用される２つの鍵K_A，K_Bを記憶している。

【００３０】暗号部１２は、制御部１１より供給されたデータを、所定の鍵で暗号化し、暗号化したデータ（暗号）を送信部１６（送信手段）に出力するようになされている。

【００３１】送信部１６は、暗号部１２より供給されたデータ（暗号）を、所定の変調方式（例えば、ＰＳＫ（Phase Shift Keying）変調方式）で変調し、生成された変調波を、アンテナ部１７を介してＩＣカード２に送信するようになされている。

【００３２】受信部１８（受信手段）は、アンテナ部１７を介して、ＩＣカード２により送信された変調波を受信し、その変調波に対応する復調方式で復調し、復調したデータ（暗号）を復号部１３に出力するようになされ

ている。

【００３３】復号部１３は、受信部１８より供給されたデータ（暗号）を、所定の鍵で復号化し、復号化したデータを制御部１１に出力するようになされている。

【００３４】図３は、図２の暗号部１２の一構成例を示している。暗号部１２においては、鍵保存部３１は、制御部１１より供給された鍵Ｋを保持するようになされている。

【００３５】データランダム化部３２は、鍵保存部３１から鍵Ｋを読み出し、その鍵Ｋで、制御部３１より供給されたデータを暗号化し、生成された暗号を送信部１６に出力するようになされている。

【００３６】図４は、図３のデータランダム化部３２の一構成例を示している。このデータランダム化部３２は、複数のインボリューション処理を行うＤＥＳ方式（例えば、「暗号と情報セキュリティ」辻井　重男、笠原　正雄　編著、１９９０年、昭晃堂に記載されている）で暗号を生成するようになされている。このデータランダム化部３２においては、鍵データ生成回路６１は、鍵保存部３１から読み出した鍵Ｋから、１６個の鍵データK_1乃至K_{16}を算出し、鍵データK_1乃至K_{16}を、演算回路６２－１乃至６２－１６にそれぞれ出力するようになされている。

【００３７】レジスタ６３は、制御部１１より供給された６４ビット（８バイト）のデータを保持し、その６４ビットのデータのうちの上位３２ビットを加算器６４－１に出力し、下位３２ビットを演算回路６２－１および加算器６４－２に出力するようになされている。

【００３８】演算回路６２－ｉ（ｉ＝１，・・・，１６）は、レジスタ６３の下位３２ビット（演算回路６２－１の場合）または加算器６４－（ｉ－１）（演算回路６２－２乃至６２－１６の場合）より供給された３２ビットのデータに対して、鍵データ生成回路６１より供給された鍵データK_iを利用して、所定の変換を行い、変換後の３２ビットのデータを加算器６４－ｉに出力するようになされている。

【００３９】加算器６４－ｉ（ｉ＝１，・・・，１６）は、レジスタ６３の上位３２ビット（加算器６４－１の場合）、レジスタ６３の下位３２ビット（加算器６４－２の場合）、および、加算器６４－（ｉ－２）（加算器６４－３乃至６４－１６の場合）のいずれかより供給された３２ビットのデータと、演算回路６２－ｉより供給された３２ビットのデータの排他的論理和（ビット毎の排他的論理和）を計算し、その排他的論理和（３２ビット）を、加算器６４－（ｉ＋２）（加算器６４－１乃至６４－１４の場合）、レジスタ６５の下位３２ビット（加算器６４－１５の場合）、および、レジスタ６５の上位３２ビット（加算器６４－１６の場合）のいずれか、並びに、演算回路６２－（ｉ＋１）（加算器６４－１乃至６４－１５の場合）に出力するようになされている。

【００４０】レジスタ６５は、加算器６４－１５より供給された３２ビットのデータを、下位３２ビットで保持し、加算器６４－１６より供給された３２ビットのデータを、上位３２ビットで保持するとともに、これらの２つの３２ビットのデータで構成される６４ビットのデータを、暗号として送信部１６に出力するようになされている。

【００４１】図５は、図２の復号部１３の一構成例を示している。この復号部１３においては、鍵保存部４１は、制御部１１より供給された鍵Ｋを保持するようになされている。

【００４２】変換部４２は、図４のデータランダム化部３２と同一の構成を有し、鍵保存部４１から鍵Ｋを読み出し、受信部１８より供給されたデータ（ＤＥＳ方式で暗号化された暗号）をレジスタ６３に供給した後、図４のデータランダム化部３２と同一の動作を行い、そのデータを復号化し、復号化したデータをレジスタ６５から制御部１１に出力するようになされている。

【００４３】図６は、本発明の一実施例であるＩＣカード２の構成例を示している。

【００４４】ＩＣカード２においては、制御部８１（処理手段）は、Ｒ／Ｗ１により供給されるコマンドに応じて、各種処理を行うようになされている。制御部８１は、Ｒ／Ｗ１からのコマンドを、復号部８３（復号化手段）から受け取り、そのコマンドに対応した処理を行い、その処理の結果に対応する応答データ（Ｒ／Ｗ１に送信するもの）を、暗号部８２（暗号化手段）に出力するようになされている。

【００４５】また、制御部８１は、メモリ８４から、暗号化または復号化に利用される鍵K_Aまたは鍵K_Bを読み出し、その鍵K_Aまたは鍵K_Bを、暗号部８２または復号部８３に出力するようになされている。

【００４６】メモリ８４は、ＲＡＭ（Random Access Memory）部（１２８キロバイト程度）とＲＯＭ（Read Only Memory）部（５１２キロバイト程度）を有している。そのうちのＲＡＭ部は、制御部８１における処理に使用されるデータなどを一時的に記憶する。一方、ＲＯＭ部には、暗号化または復号化において利用される２つの鍵K_A，K_Bが、予め記憶されている。

【００４７】暗号部８２および復号部８３は、図３の暗号部１２および図５の復号部１３と同様の構成であるので、その説明を省略する。

【００４８】送信部８６（送信手段）は、暗号部８２より供給されたデータ（暗号）を、所定の変調方式（例えば、ＰＳＫ（Phase Shift Keying）変調方式）で変調し、生成された変調波を、アンテナ部８７を介してＲ／Ｗ１に送信するようになされている。

【００４９】受信部８８（受信手段）は、アンテナ部８７を介して、Ｒ／Ｗ１により送信された変調波を受信

し、その変調波に対応する復調方式で復調し、復調したデータ（暗号）を復号部８３に出力するようになされている。

【００５０】次に、図７および図８のフローチャート、並びに、図９を参照して、Ｒ／Ｗ１とＩＣカード２の、相互認証を行うときの動作について説明する。

【００５１】最初に図７のステップＳ１において、Ｒ／Ｗ１の制御部１１は、６４ビットの乱数R_A（第１のデータ）を生成し、その乱数R_Aを暗号部１２のデータランダム化部３２に出力するとともに、メモリ１４から鍵K_Bを読み出し、暗号部１２の鍵保存部３１に出力する。

【００５２】図３の暗号部１２のデータランダム化部３２は、鍵保存部３１から鍵K_Bを読み出す。そして、図４のデータランダム化部３２の鍵データ生成回路６１は、鍵K_Bから１６個の鍵データK_1乃至K_{16}を生成し、演算回路６２－１乃至６２－１６にそれぞれ出力する。

【００５３】データランダム化部３２のレジスタ６３は、Ｒ／Ｗ１より供給された乱数R_Aの上位３２ビットを加算器６４－１に出力し、乱数R_Aの下位３２ビットを演算回路６２－１および加算器６４－２に出力する。演算回路６２－１は、その３２ビットのデータを鍵データK_1を利用して変換し、変換後のデータを加算器６４－１に出力する。加算器６４－１は、レジスタ６３より供給された３２ビットのデータと、演算回路６２－１より供給された３２ビットのデータの排他的論理和（ビット毎の排他的論理和）を計算し、その排他的論理和（３２ビット）を、演算回路６２－２および加算器６４－３に出力する。

【００５４】次に、演算回路６２－２は、その３２ビットのデータを鍵データK_2を利用して変換し、変換後のデータ（３２ビット）を加算器６４－２に出力する。加算器６４－２は、レジスタ６３より供給された３２ビットのデータと、演算回路６２－２より供給された３２ビットのデータの排他的論理和を計算し、その排他的論理和を、演算回路６２－３および加算器６４－４に出力する。

【００５５】演算回路６２－３乃至６２－１４および加算器６４－３乃至６４－１４は、順次、演算回路６２－２および加算器６４－２と同様の動作を行う。即ち、演算回路６２－ｊ（ｊ＝３，・・・，１４）は、加算器６４－（ｊ－１）より供給された３２ビットのデータを鍵データK_jを利用して変換し、変換後のデータを加算器６４－ｊに出力する。加算器６４－ｊ（ｊ＝３，・・・，１４）は、加算器６４－（ｊ－２）より供給された３２ビットのデータと、演算回路６２－ｊより供給された３２ビットのデータの排他的論理和を計算し、その排他的論理和を、演算回路６２－（ｊ＋１）および加算器６４－（ｊ＋２）に出力する。

【００５６】さらに、演算回路６２－１５は、加算器６４－１４より供給された３２ビットのデータを鍵データK_{15}を利用して変換し、変換後のデータを加算器６４－１５に出力する。加算器６４－１５は、加算器６４－１３より供給された３２ビットのデータと、演算回路６２－１５より供給された３２ビットのデータの排他的論理和を計算し、その排他的論理和を、演算回路６２－１６およびレジスタ６５の下位３２ビットに出力する。

【００５７】そして、演算回路６２－１６は、その３２ビットのデータを鍵データK_{16}を利用して変換し、変換後のデータを加算器６４－１６に出力する。加算器６４－１６は、加算器６４－１４より供給された３２ビットのデータと、演算回路６２－１６より供給された３２ビットのデータの排他的論理和を計算し、その排他的論理和を、レジスタ６５の上位３２ビットに出力する。

【００５８】以上のようにして、合計１６段の演算を行って暗号を生成する。そして、データランダム化部３２のレジスタ６５は、生成した暗号C_1（第１の暗号）（図９の［R_A］$_B$）を送信部１６に出力する。

【００５９】次に、ステップＳ２において、Ｒ／Ｗ１の送信部１６は、暗号部１２より供給された暗号C_1を変調し、生成された変調波を、アンテナ部１７を介してＩＣカード２に送信する。

【００６０】このように、Ｒ／Ｗ１が、ステップＳ１，Ｓ２において処理を行い、変調波を送信するまでの間、ＩＣカード２は、図８のステップＳ２１において待機している。

【００６１】そして、Ｒ／Ｗ１から変調波が送信されてくると、ＩＣカード２の受信部８８は、アンテナ部８７を介して、Ｒ／Ｗ１の送信部１６により送信された変調波を受信し、その変調波を復調し、復調後のデータ（暗号C_1）を復号部８３に出力する。

【００６２】次に、ステップＳ２２において、ＩＣカード２の復号部８３の変換部４２は、予め制御部８１より鍵保存部４１に供給されている鍵K_Bで、受信部８８より供給された暗号C_1を復号化し、復号化したデータ（平文M_1）（第２のデータ）を制御部８１に出力する。

【００６３】ステップＳ２３において、ＩＣカード２の制御部８１は、復号部８３より供給された平文M_1を、暗号部８２のデータランダム化部３２に出力する。暗号部８２のデータランダム化部３２は、鍵保存部３１に予め記憶されている鍵K_Aを読み出し、その鍵K_Aで、ステップＳ１におけるＲ／Ｗ１の暗号部１２のデータランダム化部３２と同様に、平文M_1を暗号化し、生成された暗号C_2（第２の暗号）（図９の［R_A］$_A$）を送信部８６に出力する。

【００６４】また、制御部８１は、乱数R_B（第３のデータ）を生成し、その乱数R_Bを暗号部８２のデータランダム化部３２に出力する。暗号部８２のデータランダム化部３２は、鍵保存部３１から鍵K_Aを読み出し、そ

17

の鍵K_Aで乱数R_Bを暗号化し、生成された暗号C_3（第３の暗号）（図９の［R_B］$_A$）を送信部８６に出力する。

【００６５】そして、ステップＳ２４において、ＩＣカード２の送信部８６は、暗号C_2，C_3を変調し、生成された変調波を、アンテナ部８７を介してＲ／Ｗ１に送信する。

【００６６】このように、ＩＣカード２がステップＳ２１乃至Ｓ２４の処理を行っている間、Ｒ／Ｗ１は、図７のステップＳ３およびステップＳ４において、ＩＣカード２から暗号C_2と暗号C_3が送信されてくるまで待機するとともに、暗号C_1を送信してからの経過時間を、ステップＳ３において監視し、ＩＣカード２からC_2とC_3が送信されてくるまでに所定の時間（ＩＣカード２における処理に通常要する時間より長い時間）が経過した場合、ステップＳ２に戻り、暗号C_1を再送する。

【００６７】そして、ＩＣカード２から暗号C_2および暗号C_3を含む変調波が送信されてくると、Ｒ／Ｗ１に受信部１８は、アンテナ部１７を介して、ＩＣカード２の送信部８６により送信された変調波を受信し、その変調波を復調する。そして、受信部１８は、復調されたデータ（暗号C_2，C_3）を、復号部１３に出力する。

【００６８】次に、ステップＳ５において、Ｒ／Ｗ１の復号部１３の変換部４２は、鍵保存部４１に予め供給されている鍵K_Aを読み出し、受信部１８より供給されたデータ（暗号C_2，C_3）を復号化し、復号化したデータ（平文M_2（暗号C_2に対応する）（第４のデータ）と平文M_3（暗号C_3に対応する）（第５のデータ））を制御部１１に出力する。

【００６９】そして、ステップＳ６において、Ｒ／Ｗ１の制御部１１は、平文M_2と乱数R_Aが同一であるか否かを判断し、平文M_2と乱数R_Aが同一であると判断した場合、ステップＳ７において、Ｒ／Ｗ１は、ＩＣカード２がＲ／Ｗ１の鍵K_A，K_Bと同一の鍵K_A，K_Bを有していると判断し、ＩＣカード２を認証する。

【００７０】一方、ステップＳ６において、平文M_2と乱数R_Aが同一ではないと判断した場合、Ｒ／Ｗ１は、ＩＣカード２を認証しないので、認証処理を終了する。

【００７１】ステップＳ７においてＩＣカード２を認証した後、ステップＳ８において、Ｒ／Ｗ１の制御部１１は、ステップＳ５で生成した平文M_3を暗号部１２に出力する。そして、暗号部１２は、ステップＳ１と同様に、平文M_3を鍵K_Bで暗号化し、生成された暗号C_4（第４の暗号）（図９の［R_B］$_B$）を送信部１６に出力する。

【００７２】ステップＳ９において、Ｒ／Ｗ１の送信部１６は、暗号部１２より供給された暗号C_4を変調し、生成された変調波を、アンテナ部１７を介してＩＣカード２に送信する。

【００７３】このように、Ｒ／Ｗ１が、ステップＳ４乃至Ｓ９において処理を行っている間、ＩＣカード２は、図８のステップＳ２５およびステップＳ２６において、暗号C_4が送信されてくるまで待機している。このとき、ＩＣカード２の制御部８１は、暗号C_2，C_3を送信してからの経過時間を監視しており、ステップＳ２６において暗号C_2，C_3を送信してから所定の時間が経過したと判断した場合、Ｒ／Ｗ１を認証せずに認証処理を終了する。

18

【００７４】一方、暗号C_4を含む変調波が送信されてくると、ＩＣカード２の受信部８８は、Ｒ／Ｗ１により送信された変調波を、アンテナ部８７を介して受信し、その変調波を復調する。そして、受信部８８は、復調したデータ（暗号C_4）を復号部１３に出力する。

【００７５】次にステップＳ２７において、ＩＣカード２の復号部８３の変換部４２は、鍵保存部４１から読み出した鍵K_Bで、受信部８８より供給されたデータ（暗号C_4）を復号化し、復号化したデータ（平文M_4）（第６のデータ）を制御部８１に出力する。

【００７６】そして、ステップＳ２８において、ＩＣカード２の制御部８１は、平文M_4と乱数R_Bが同一であるか否かを判断し、平文M_4と乱数R_Bが同一であると判断した場合、ステップＳ２９において、ＩＣカード２は、Ｒ／Ｗ１がＩＣカード２の鍵K_A，K_Bと同一の鍵K_A，K_Bを有していると判断し、Ｒ／Ｗ１を認証する。

【００７７】一方、ステップＳ２８において、平文M_4と乱数R_Bが同一ではないと判断した場合、ＩＣカード２は、Ｒ／Ｗ１を認証しないので、認証処理を終了する。

【００７８】以上のようにして、Ｒ／Ｗ１は、図７に示すように、ＩＣカード２に対する認証処理を行い、ＩＣカード２は、図８に示すように、Ｒ／Ｗ１に対する認証処理を行うことにより、相互に、認証処理を行う。

【００７９】なお、上述の暗号部１２，８２のデータランダム化部３２は、ＤＥＳ方式で暗号化を行っているが、他の方式（例えば、ＦＥＡＬ（Fast Encryption Algorithm）－８方式）で暗号化を行うようにしてもよい。その場合、復号部１３，８３の変換部４２は、その暗号化方式に対応して復号化を行うようにする。

【００８０】また、ＦＥＡＬ－８方式を利用した場合、３５ミリ秒程度（ＩＣカード２における処理にかかる時間は２８ミリ秒程度）で相互認証を行うことができる。

【００８１】次に、図１０および図１１のフローチャートを参照して、上述の認証処理後（相互に認証した後）におけるＲ／Ｗ１とＩＣカード２間の通信について説明する。

【００８２】図１０のステップＳ４１において、Ｒ／Ｗ１の制御部１１は、最初に、上述の認証処理における乱数R_Aを認識番号ＩＤとして保持するとともに、乱数R_B（平文M_3）（ＩＣカード２を認証したので、Ｒ／Ｗ１は、平文M_3を乱数R_Bとする）を新たな鍵K_{10}（第３の

鍵）として、暗号部１２の鍵保存部３１および復号部１３の鍵保存部４１に出力する。

【００８３】そして、Ｒ／Ｗ１の制御部１１は、ＩＣカード２に実行させる処理に対応するコマンド（送信コマンド）を、暗号部１２のデータランダム化部３２に出力する。暗号部１２のデータランダム化部３２は、鍵保存部３１から鍵K_{ID}を読み出し、その鍵K_{ID}で送信コマンドを暗号化し、生成された暗号Ccom（第５の暗号）を送信部１６に出力する。

【００８４】また、Ｒ／Ｗ１の制御部１１は、認識番号ＩＤを、暗号部１２のデータランダム化部３２に出力する。暗号部１２のデータランダム化部３２は、鍵K_{ID}で認識番号ＩＤを暗号化し、生成された暗号C_{ID}（第６の暗号）を送信部１６に出力する。

【００８５】ステップＳ４２において、Ｒ／Ｗ１の送信部１６は、暗号部１２より供給された暗号Ccom，C_{ID}を変調し、生成された変調波をアンテナ部１７を介してＩＣカード２に送信する。

【００８６】このように、Ｒ／Ｗ１が、暗号Ccom，C_{ID}を含む変調波を送信するまでの間、ＩＣカード２は、図１１のステップＳ６１において待機している。

【００８７】なお、ＩＣカード２の制御部８１は、上述の認証処理における乱数Raを鍵K_{ID}として、予め、暗号部８２の鍵保存部３１および復号部８３の鍵保存部４１に出力するとともに、乱数R_A（平文M_1）（Ｒ／Ｗ１を認証したので、ＩＣカード２は、平文M_1を乱数R_Aとする）を認識番号ＩＤとして保持している。

【００８８】そして、Ｒ／Ｗ１から暗号Ccom，C_{ID}を含む変調波を送信されてくると、ＩＣカード２の受信部８８は、Ｒ／Ｗ１の送信部１６により送信された変調波を、アンテナ部８７を介して受信し、その変調波を復調する。そして、受信部８８は、復調したデータ（暗号Ccom，C_{ID}）を、復号部８３に出力する。

【００８９】ステップＳ６２において、復号部８３の変換部４２は、鍵保存部４１に予め記憶されている鍵K_{ID}で、供給されたデータのうちの暗号C_{ID}を復号化し、復号されたデータ（平文M_{ID}）（第７のデータ）を制御部８１に出力する。

【００９０】そして、ステップＳ６３において、ＩＣカード２の制御部８１は、平文M_{ID}の値が認識番号ＩＤ以上であるか否かを判断し、平文M_{ID}の値が認識番号ＩＤより小さいと判断した場合、通信処理を終了する。一方、平文M_{ID}の値が認識番号ＩＤ以上であると判断した場合、ステップＳ６４において、制御部８１は、送信されてきたコマンド（暗号Ccom）を承認し、復号部８３に、暗号Ccomを復号化させ、ステップＳ６５において、復号化したコマンドに対応する処理を行い、ステップＳ６６において、その処理結果に対応する応答データ（Ｒ／Ｗ１に送信するためのもの）を作成する。

【００９１】次に、ステップＳ６７において、ＩＣカード２の制御部８１は、認識番号ＩＤの値を１だけ増加させた後、認識番号ＩＤおよび応答データを、暗号部８２に順次出力する。ステップＳ６８において、暗号部８２は、認識番号ＩＤを、鍵K_{ID}で暗号C_{ID}（第８の暗号）に暗号化するとともに、応答データを、鍵K_{ID}で暗号Cre（第７の暗号）に暗号化した後、暗号C_{ID}および暗号Creを、送信部８６に出力する。

【００９２】そして、ステップＳ６９において、送信部８６は、暗号C_{ID}と暗号Creを変調し、生成した変調波をＲ／Ｗ１に送信する。

【００９３】このように、ＩＣカード２がステップＳ６１乃至Ｓ６９において送信したコマンドに対応する処理を行っている間、Ｒ／Ｗ１は、ステップＳ４３およびステップＳ４４において待機するとともに、暗号C_{ID}，Ccomを送信した時からの経過時間をステップＳ４３において監視する。

【００９４】そして、予め設定されている所定の時間が経過すると、ステップＳ４５に進み、制御部１１は、ステップＳ４１で暗号化したコマンドと同一のコマンドを選択し、ステップＳ４６で、認識番号ＩＤの値を１だけ増加させた後、ステップＳ４１に戻り、送信コマンドと認識番号ＩＤを暗号化し、ステップＳ４２において、生成された暗号をＩＣカード２に再送する。

【００９５】一方、ステップＳ４４において、ＩＣカード２からの暗号C_{ID}と暗号Creを含む変調波が送信されてくると、Ｒ／Ｗ１に受信部１８が、その変調波を、暗号C_{ID}と暗号Creに復調し、その暗号C_{ID}と暗号Creを復号部１３に出力する。

【００９６】ステップＳ４７において、復号部１３は、暗号C_{ID}を鍵K_{ID}で復号化し、生成された平文M_{ID}（第９のデータ）を制御部１１に出力する。

【００９７】ステップＳ４８において、制御部１１は、平文M_{ID}の値が、認識番号ＩＤより大きいか否かを判断し、平文M_{ID}の値が認識番号ＩＤ以下であると判断した場合、ステップＳ４５に進み、ステップＳ４１で送信したコマンドと同一のコマンドを選択し、ステップＳ４６において、認識番号ＩＤの値を１だけ増加させた後、ステップＳ４１に戻り、送信コマンドと認識番号ＩＤを暗号化し、ステップＳ４２において、生成された暗号をＩＣカード２に再送する。

【００９８】一方、ステップＳ４８において、平文M_{ID}の値が、認識番号ＩＤより大きいと判断した場合、制御部１１は、ステップＳ４９において、復号部１３に、暗号Creを復号化させ、ＩＣカード２からの応答データを受け取る。

【００９９】そして、ステップＳ５０において、Ｒ／Ｗ１の制御部１１は、通信を終了するか否かを判断する。通信を継続する場合、ステップＳ５１に進み、Ｒ／Ｗ１の制御部１１は、次の送信コマンドを選択する。

【０１００】そして、ステップＳ４６に進み、認識番号

21

ＩＤの値を１だけ増加させた後、ステップＳ４１に戻り、ステップＳ４１以降で、次の送信コマンドの送信を行う。

【０１０１】以上のようにして、相互認証時に送信した乱数R_A，R_Bを、認識番号ＩＤおよび新たな鍵K_{ID}として利用して、Ｒ／Ｗ１は、ＩＣカード２に所定のコマンドを送信し、ＩＣカード２は、そのコマンドに対応する処理を行った後、その処理結果に対応する応答データをＲ／Ｗ１に送信する。このようにすることにより、認識番号および新たな鍵を利用して、通信毎に、通信相手が正規の者であることを確認することができる。また、１回の通信毎に認識番号ＩＤの値を１ずつ増加させているので、現在までの通信回数を知ることができ、処理の経過を把握することができる。

【０１０２】なお、ステップＳ６３において、ＩＣカード２の制御部８１は、平文M_{ID}が認識番号ＩＤ以上であるか否かを判断しているが、平文M_{ID}の値が認識番号ＩＤに対応する所定の範囲内（例えば、ＩＤ乃至ＩＤ＋１６の範囲）の値と同一であるか否かを判断するようにしてもよい。このようにすることにより、例えば、伝送路に障害が生じ、Ｒ／Ｗ１が放射した電磁波（認識番号の値がＩＤ）がＩＣカード２に到達しなかった場合において、ＩＣカード２は、次に送信されてくるデータ（認識番号の値はＩＤ＋１であるが、送信コマンドは、前回送信したコマンドと同一である）を受信することができる。

【０１０３】あるいは、ステップＳ６３において、ＩＣカード２の制御部８１は、平文M_{ID}（６４ビット）の例えば下位８ビットの値が、認識番号ＩＤの下位８ビットの値以上であるか否かを判断するようにしてもよい。このように所定の桁数（ビット数）ｎだけにおいて比較を行うことにより、６４ビットにおいて比較を行う場合より、ビット演算量が減少し、処理を速く行うことができる。なお、この場合、認識番号ＩＤの値が2^n-1（ｎは桁数）より大きくなると桁上がりが発生する（比較の結果にエラーが生じる）ので、Ｒ／Ｗ１とＩＣカード２の間の通信の回数を考慮して、認識番号ＩＤの値が2^n-1（ｎは桁数）より大きくならないように、桁数ｎを設定する。

【０１０４】また、同様に、ステップＳ４８において、Ｒ／Ｗ１の制御部１１は、平文M_{ID}の値が認識番号ＩＤに対応する所定の範囲内の値と同一であるか否かを判断するようにしてもよい。また、ステップＳ４８において、Ｒ／Ｗ１の制御部１１は、平文M_{ID}の例えば下位８ビットの値が、認識番号ＩＤの下位８ビットの値より大きいか否かを判断するようにしてもよい。

【０１０５】なお、上記実施例においては、乱数R_Bを新たな鍵K_{ID}としているが、図１２に示すように乱数R_Aと乱数R_Bから新たな鍵K_{ID}を算出し、その鍵K_{ID}を利用して通信を行うようにしてもよい。

22

【０１０６】また、Ｒ／Ｗ１が送信した情報を、ＩＣカード２に、単に記憶しておく場合、図１３に示すように、ＩＣカード２は、受信したデータ（鍵K_Aまたは鍵K_Bで暗号化されたデータ）を、復号化せずに、そのままメモリ８４に記憶させておき、Ｒ／Ｗ１からのリードコマンドを受け取ったときに、そのデータをメモリ８４から読み出し、そのまま送信するようにしてもよい。

【０１０７】

【発明の効果】以上のごとく、請求項１に記載の認証方法によれば、第１の情報処理装置が、第１のデータを第１の暗号に暗号化し、第２の情報処理装置が、第１の暗号を第２のデータに復号化し、その第２のデータを第２の暗号に暗号化するとともに、第３のデータを第３の暗号に暗号化し、第１の情報処理装置が、第２の暗号を第４のデータに復号化し、第１の情報処理装置が、第１のデータと第４のデータに応じて、第２の情報処理装置を認証する。そして、第１の情報処理装置が、第３の暗号を第５のデータに復号化し、その第５のデータを第４の暗号に暗号化し、第２の情報処理装置が、第４の暗号を第６のデータに復号化し、第２の情報処理装置が、第３のデータと第６のデータに応じて、第１の情報処理装置を認証するようにしたので、２つの情報処理装置が相互に認証を行うことができる。

【０１０８】請求項２に記載の通信方法によれば、第１の情報処理装置が、第１のデータを暗号化した第１の暗号を、第２の情報処理装置に送信し、第２の情報処理装置が、第１の暗号を受信し、その第１の暗号を第２のデータに復号化するとともに、その第２のデータを暗号化した第２の暗号と、第３のデータを暗号化した第３の暗号を、第１の情報処理装置に送信し、第１の情報処理装置が、第２の暗号および第３の暗号を受信し、そのうちの第２の暗号を第４のデータに復号化し、第１の情報処理装置が、第１のデータと第４のデータに応じて、第２の情報処理装置を認証する。そして、第１の情報処理装置が、第３の暗号を第５のデータに復号化するとともに、第５のデータを暗号化した第４の暗号を、第２の情報処理装置に送信し、第２の情報処理装置が、第４の暗号を受信し、その第４の暗号を第６のデータに復号化するとともに、第３のデータと第６のデータに応じて、第１の情報処理装置を認証するようにしたので、相互に認証した２つの情報処理装置で通信を行うことができる。

【０１０９】請求項１５に記載の情報処理装置によれば、暗号化手段が、第１の鍵で、第１のデータを第１の暗号に暗号化し、送信手段が、第１の暗号を他の情報処理装置に送信し、受信手段が、他の情報処理装置から、第２の暗号および第３の暗号を受け取り、復号化手段が、第２の暗号を、第２の鍵で第４のデータに復号化するとともに、第３の暗号を、第２の鍵で第５のデータに復号化し、認証手段が、第１のデータと第４のデータに応じて、他の情報処理装置を認証し、暗号化手段が、第

23

５のデータを、第１の鍵で第４の暗号に暗号化し、送信手段が、第４の暗号を他の情報処理装置に送信するようにしたので、所定の情報処理装置の認証を行うとともに、その情報処理装置により認証されることが可能となる。

【０１１０】請求項２４に記載の情報処理装置によれば、受信手段が、他の情報処理装置により第１の暗号を受け取り、復号化手段が、第１の暗号を、第１の鍵で第１のデータに復号化し、暗号化手段が、第１のデータを、第２の鍵で第２の暗号に暗号化するとともに、第２のデータを、第２の鍵で第３の暗号に暗号化し、送信手段が、第２の暗号および第３の暗号を他の情報処理装置に送信し、受信手段が、他の情報処理装置から第４の暗号を受け取り、復号化手段が、第４の暗号を、第２の鍵で第３のデータに復号化し、認証手段が、第２のデータと第３のデータに応じて、他の情報処理装置を認証するようにしたので、所定の情報処理装置の認証を行うとともに、その情報処理装置により認証されることが可能となる。

【図面の簡単な説明】

【図１】Ｒ／Ｗ１とＩＣカード２により構成される非接触カードシステムの一例を示す図である。

【図２】本発明の一実施例であるＲ／Ｗ１の構成を示すブロック図である。

【図３】図２の暗号部１２の構成例を示すブロック図である。

【図４】図３のデータランダム化部３２の構成例を示すブロック図である。

【図５】図２の復号部１３の構成例を示すブロック図である。

【図６】本発明の一実施例であるＩＣカード２の構成を

24

示すブロック図である。

【図７】図１のＲ／Ｗ１の相互認証時の動作について説明するフローチャートである。

【図８】図１のＩＣカード２の相互認証時の動作について説明するフローチャートである。

【図９】図１の非接触カードシステムの相互認証時の動作について説明する図である。

【図１０】図１のＲ／Ｗ１の通信時の処理について説明するフローチャートである。

【図１１】図１のＩＣカード２の通信時の処理について説明するフローチャートである。

【図１２】Ｒ／Ｗ１とＩＣカード２との通信の他の例を示す図である。

【図１３】Ｒ／Ｗ１とＩＣカード２との通信のさらに他の例を示す図である。

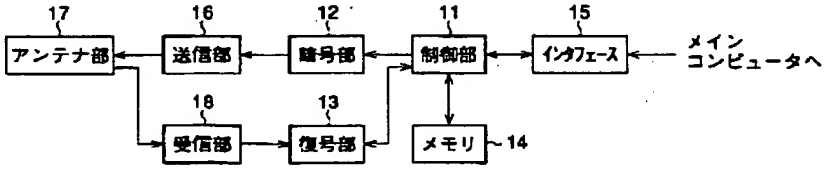
【図１４】秘密暗号を利用した通信の一例を示すブロック図である。

【図１５】秘密暗号を利用した認証の一例を示すブロック図である。

【符号の説明】

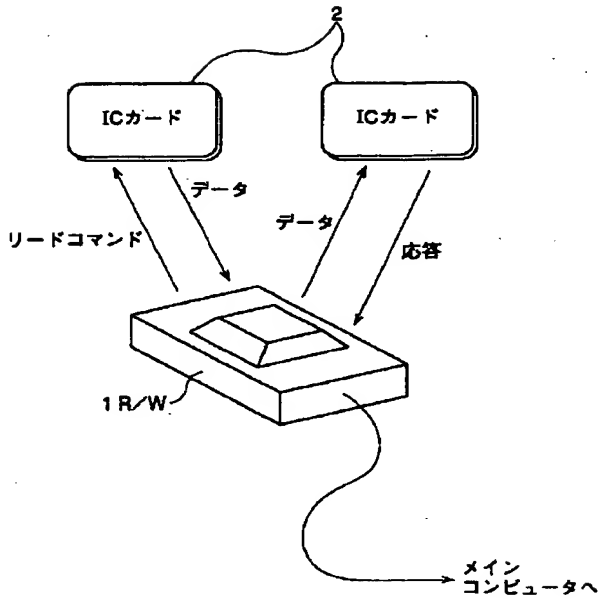
１　リーダ／ライタ（Ｒ／Ｗ），　２　ＩＣカード，　１１　制御部，　１２暗号部，　１３　復号部，　１４　メモリ，　１５　インタフェース，　１６送信部，　１７　アンテナ部，　１８　受信部，　３１　鍵保存部，　３２データランダム化部，　４１　鍵保存部，　４２　変換部，　６１　鍵データ生成回路，　６２－１乃至６２－１６　演算回路，　６３　レジスタ，　６４－１乃至６４－１６　加算器，　６５　レジスタ，　８１　制御部，　８２　暗号部，　８３　復号部，　８４　メモリ，　８６　送信部，　８７　アンテナ部，　８８　受信部

【図２】

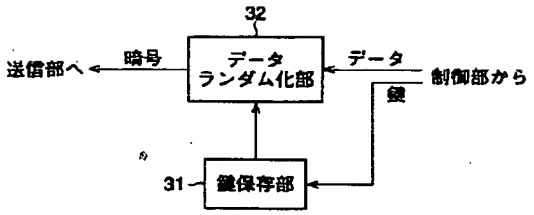


R/W 1

【図１】

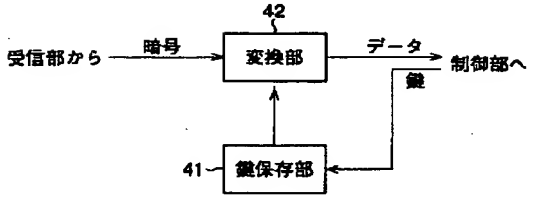


【図３】



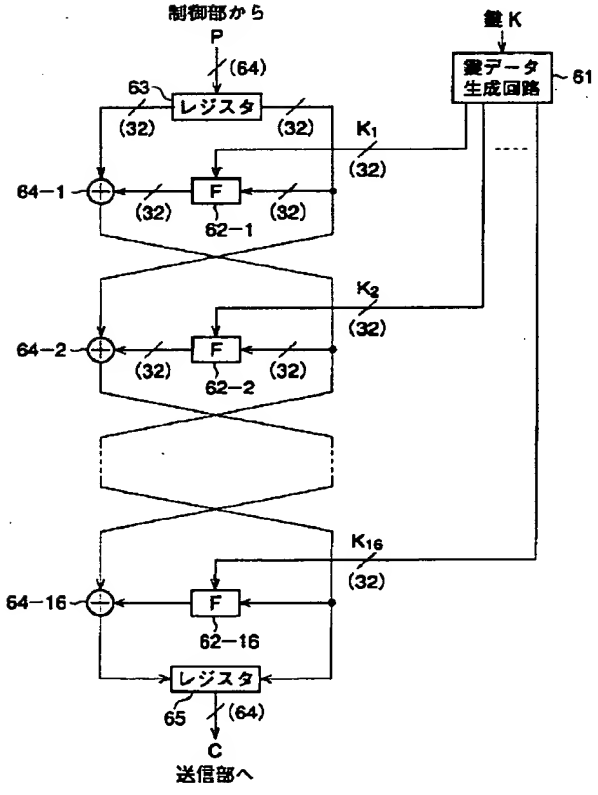
暗号部 12

【図５】

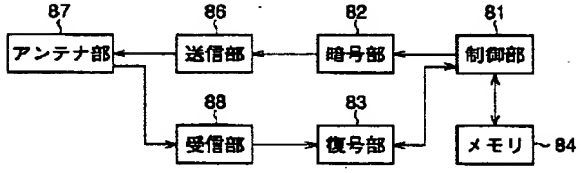


復号部 13

【図４】

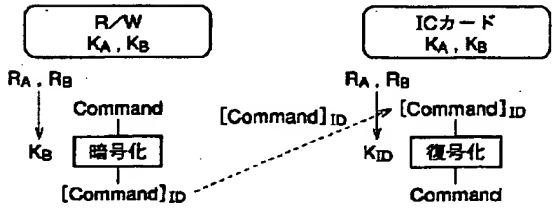


【図６】

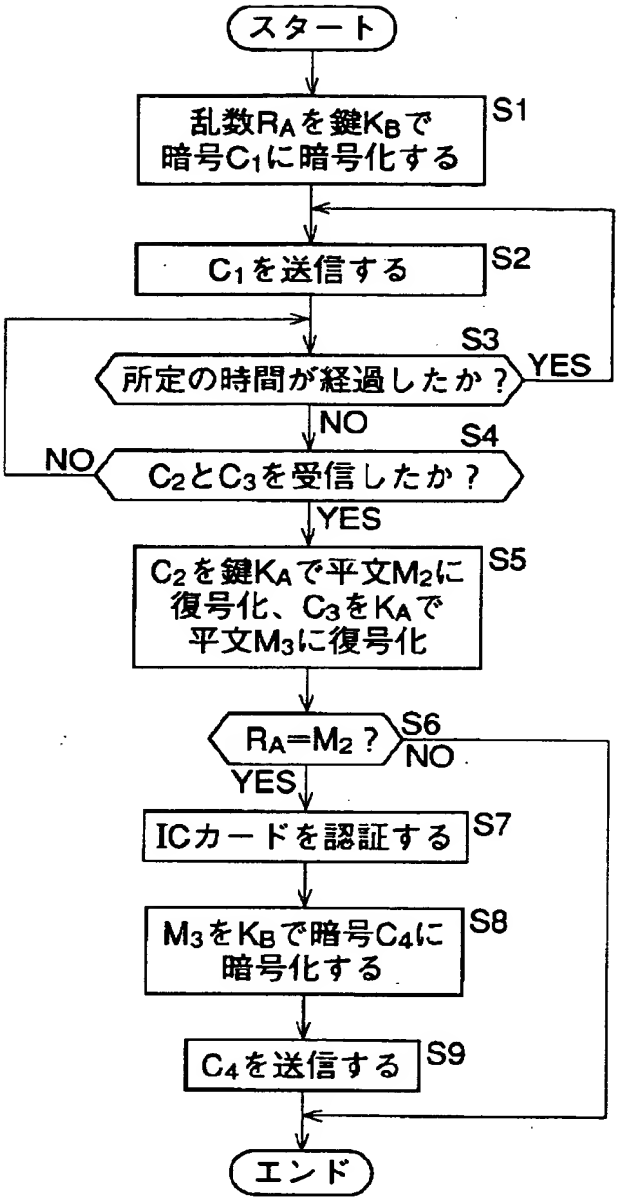


ICカード

【図１２】

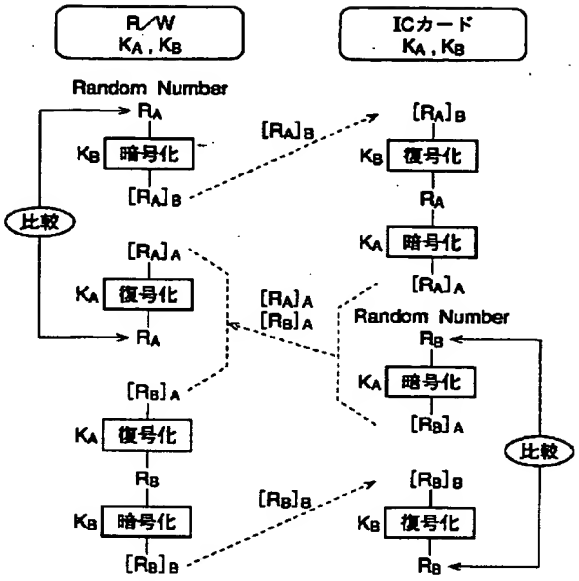


【図７】

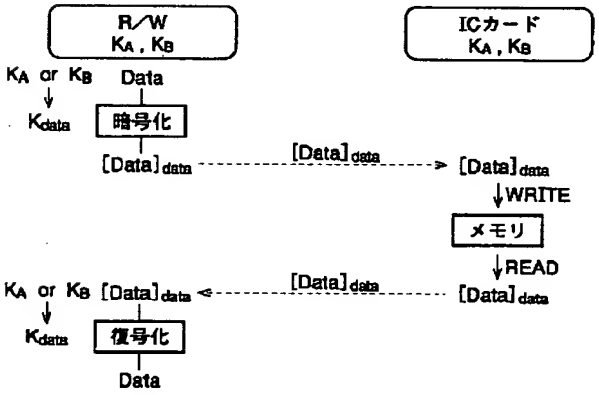


R／W1における認証処理

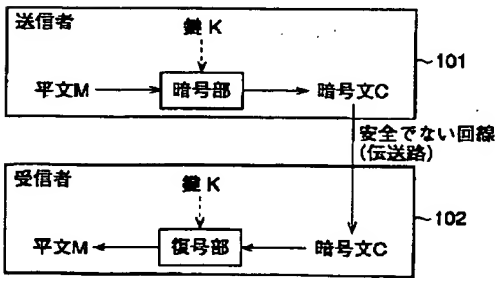
【図９】



【図１３】

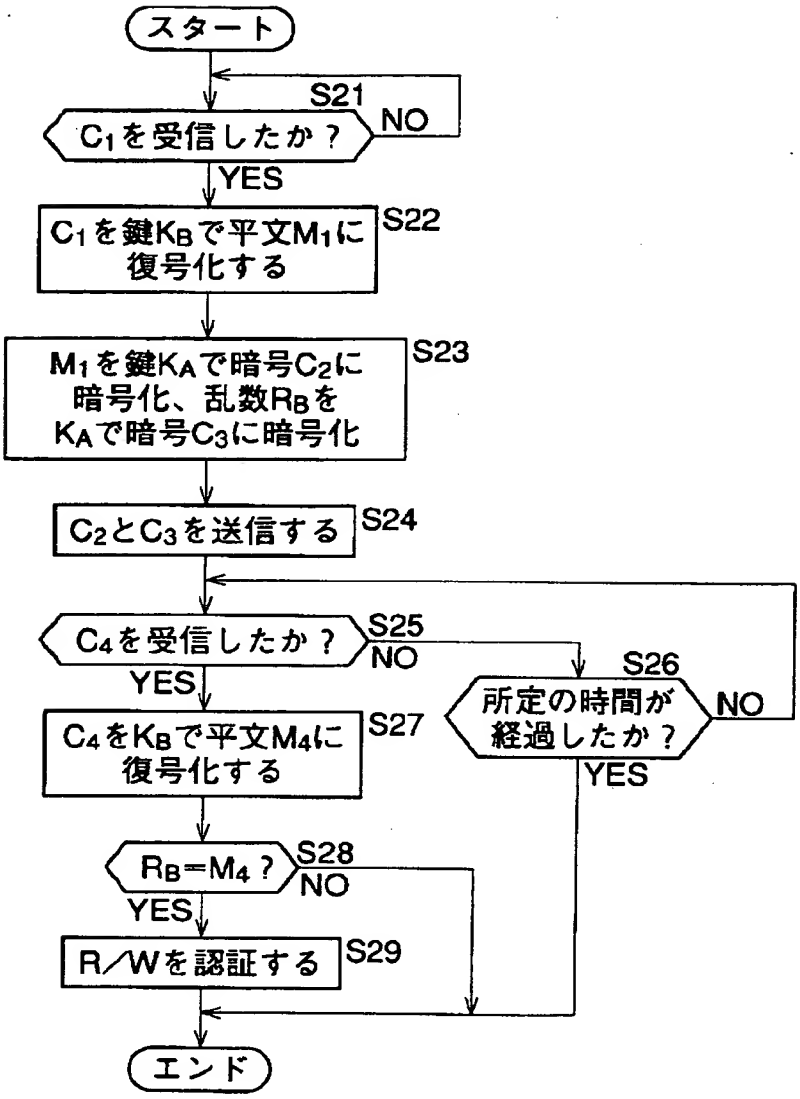


【図１４】



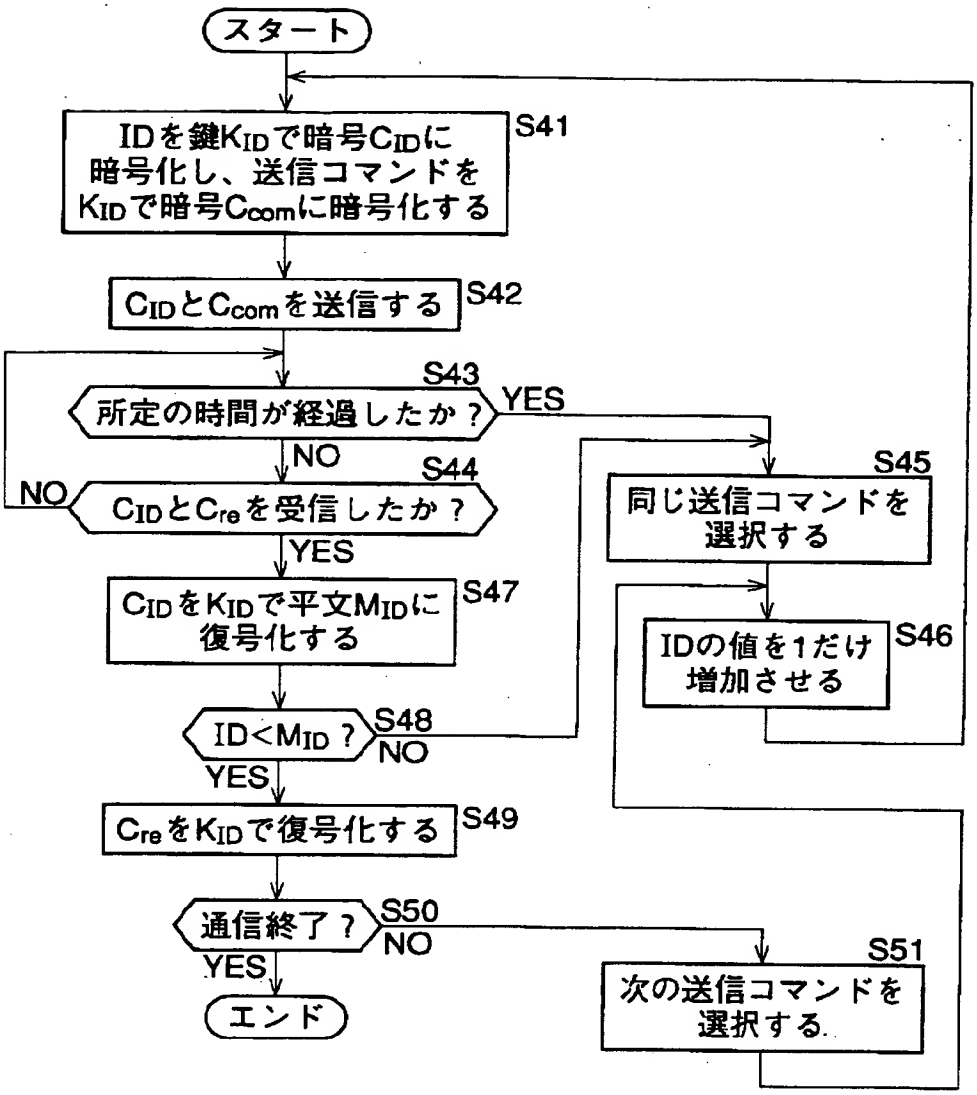
秘密通信

【図８】



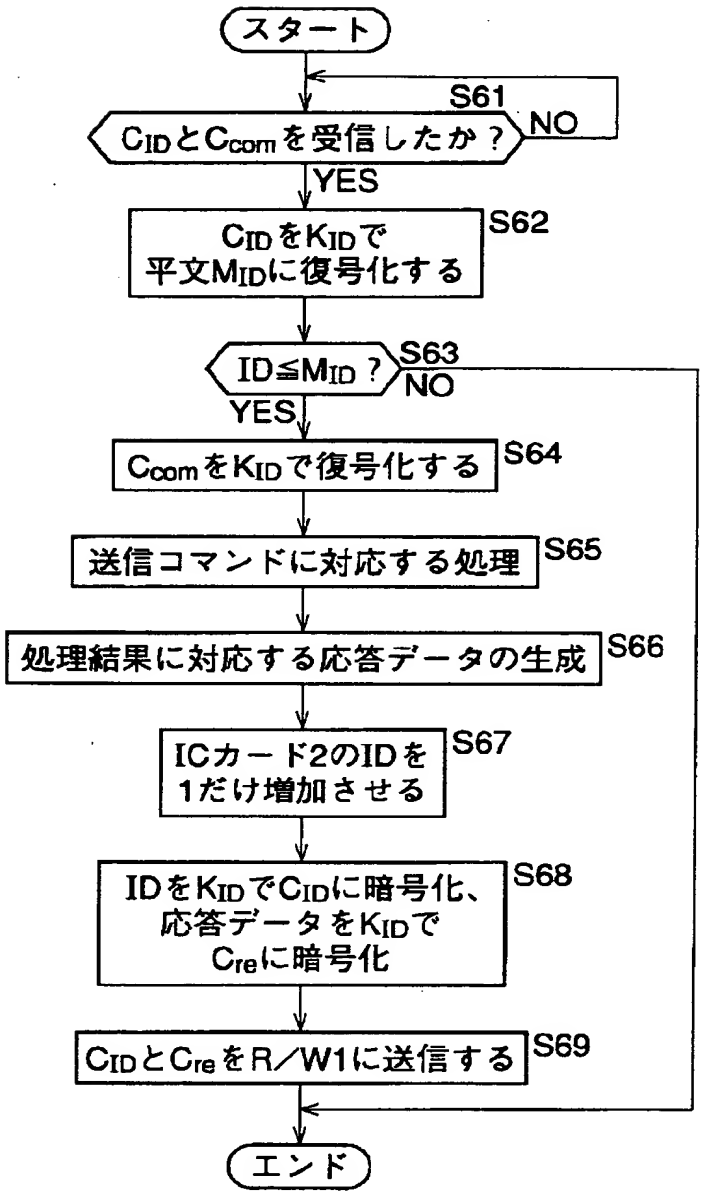
ICカードにおける認証処理

【図１０】



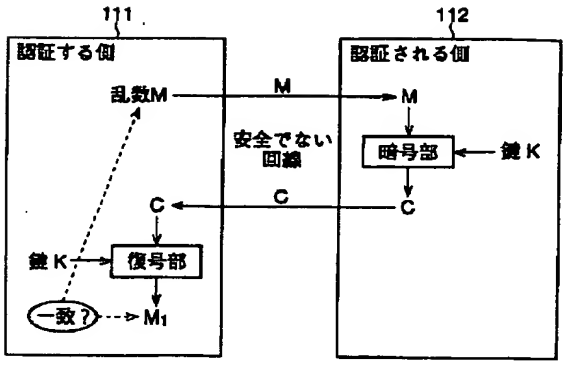
R／Wにおける処理

【図１１】



ICカードにおける処理

【図１５】



認証